UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND VIRGINIA

ROBERT DAVID STEELE, Plaintiff, -against- JASON GOODMAN, Defendant.	**17-CV-00601-MHL** **MEMORANDUM OF LAW TO SUPPORT INTERVENOR APPLICANT'S MOTION FOR INJUNCTIVE RELIEF**

MEMORANDUM OF LAW TO SUPPORT INTERVENOR APPLICANT'S AMENDED MOTION TO INTERVENE

D. GEORGE SWEIGERT is seeking the LEAVE OF THE COURT TO MOTION FOR INJUNCTIVE RELIEF pursuant to Fed. R. Civ. Proc. Rule 65(d)(c) and Va. Code Ann. § 18.2-500.

Pursuant to Local Rule 83.1(M) I swear that no attorney assisted in the preparation of the attached materials. Dated this 26th day of April, 2019.

Respectfully submitted,

Pro Se Party D. George Sweigert, c/o
P.O. Box 152
Mesa, AZ 85211
Spoliation-notice@mailbox.org

This page intentionally left blank

TABLE OF CONTENTS

TABLE OF CONTENTS 3

TABLE OF AUTHORITIES 4

INTRODUCTION 8

BACKGROUND 10

PROCEDURAL HISTORY 16

FACTUAL ALLEGATIONS 16

LAW AND ARGUMENT 23

RELIEF REQUESTED 46

TABLE OF AUTHORITIES

Cases

Balboa Island Village Inn, Inc. v. Lemen (2007) 40 Cal.4th 1141, the California Supreme Court 9

Bingham v. Strave, 184 A.D.2d 85, 89-90 (1st De't 1992) 26

Blackwelder Furniture Co. of Statesville v. Seilig Manufacturing Co., 550 F.2d 189 (4th Cir. 1977) at 195 23

Blackwelder Furniture Co. of Statesville, Inc. v. Seilig Mfg. Co., Inc., 550 F.2d 189 (4th Cir. 1977). 23

Catalano v. Pechous, 69 Ill.App.3d 797, 25 Ill.Dec. 838, 387 N.E.2d 714 (1978) 38

Central Hudson Gas & Electric Corp. v. Public Service Commission Of New York, No. 79-565, 447 U.S. 557; 100 S. Ct. 2343; 1980 U.S. LEXIS 48; 65 L. Ed. 2d 341; 6 Media L. Rep. 1497; 34 P.U.R.4th 178, June 20, 1980 39

***Chaves** v. Johnson*, **335 S.E.2d** 97 (1985) at 102 38

Copelands' Enterprises Inc. v. CNV Inc., 945 F.2d 1563, 20 USPQ2d 1295 (Fed. Cir. 1991) 22

Covucci v. Keane Consulting Group, Inc., 2006 Mass. Super LEXIS 313 (Mass. Sup. Ct. May 31, 2006) 20

Curtis Publishing Co. v. Butts, 388 U.S. 130, 87 S. Ct. 1975, 18 L. Ed. 2d 1094 (1966) 77

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993) 13

Direx Israel, Ltd. V. Breakthrough Med. Corp., 952 F.2d 802, 812 (4th Cir. 1991) 23

Esskay Art Galleries v. Gibbs, 205 Ark. 1157, 172 S.W.2d 924 27

Federal Trade Commission v. Wyndham Worldwide Corporation, et. al., 2:13-CV-01887-EAS-JAD. U.S.D.C., Dist. of New Jersey 29

Fitchette v. Taylor, 191 Minn. 582, 254 N.W. 910, 94 A.L.R. 356 27

Fleming v. Moore, 221 Va. 884, 275, S.E.2d 632, 636 (1981) 38

Fleming, 275 S.E.2d at 636 38

Frye v. United States, 293 F. 1013 (D.C. Cir. 1923) 14

FTC v. Wyndham 29

Fuller v. Edwards, 180 Va. 191, 197, 22 S.E.2d 26, 29 (1942) 27

Gazette, Inc. v. Harris, 325 S.E.2d 713 (1985) 27

Great Coastal Express v. Ellingon, 230 Va. 142, 334 S.E.2d 846, 849 (1985) 38

Mazurek v. Armstrong (96-1104), 520 U.S. 968 (1997) 37

Montgomery County Bar Ass'n v. Rinalducci, 329 Pa. 296, 197 A. 924 27

Nease v. Ford Motor Co., No. 15-1950 (4th Cir. 2017) 14

Ohralik v. Ohio State Bar Assn., 436 U.S. 447 (1978) at 462 41

Ohralik v. Ohio State Bar Assn., 436 U.S., at 457 22

Oliman v. Evans, 750 F.2d 970, 982 (D.C. Cir. 1984) 38

Rinaldi v. Holt, Rinehart & Winston, Inc., 42 N.Y.2d 369, 397 N.Y.S.2d 943, 366 N.E.2d 1299 (1977) 38

Rosenblatt v. Baer, 383 U.S. 75, 86, 86 S. Ct. 669, 676, 15 L. Ed. 2d 597 (1966) 28

Rum Creek Coal Sales, Inc. v. Capetron, 926 F,2d 353, 359 (4th Cir. 1991) 23

Shupe v. Rose's Stores, 213 Va. 374, 375-76, 192 S.E.2d 766, 767 (1972) 9, 25

Slawik v. News-Journal, 428 A.2d 15 (Del.1981) 38

Sloan v. Mitchell, 113 W.Va. 506, 168 S.E. 800 27

Unger v. Landlords' Management Corporation,114 N.J.Eq. 68, 168 A. 229 27

United States v. Verdugo-Urquidez, 494 U.S. 259 ..... 7, 15, 39

Va. Pharmacy Bd. v. Va. Consumer Council, 425 U.S. 748 (1976) at 771-772 22

Virginia v. Black, 538 U.S. 343, 358 (2003) 43

Weiss v. Levine, 133 N.J.Eq. 441, 32 A.2d 574 27

Statutes

AMENDMEMT I 39

AMENDMENT I 38, 39

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 19

E-Government Act of 2002, Public Law 107-347 42

Electronic Signatures in Global and National Commerce Act (E-Sign Act) 34, 42

Federal Information Security and *Modernization* Act of *2014, Public Law 113-283* 42

Government Paperwork Elimination Act (GPEA), Public Law 105-277 (codified at 44 U.S.C. 3504) 42

Other Authorities

Department of Justice: Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies (November 2000) 42

National Archives and Records Administration: Records Management Guidance for Agencies Implementing Electronic Signature Technologies (October 18, 2000) 42

National Institute of Standards and Technology (NIST) SP 800-63, Electronic Authentication Guideline 43

OMB M-00-10: OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act (April 25, 2000) 42

U.S. Department of State Guidebook for the Implementation of Electronic Signatures, ... 43

Rules

F.R.E. Rule 702 14

Fed. R. Civ. Proc. Rule 65(d)(C) 7

Federal Rules of Evidence 7

Federal Rules of Evidence Rule 702 14

Treatises

"*Are EVL Teachers Hiring CAI Scrubs To Hide Signals From High Value Target & Death Pool Crime Scenes?*", April 19, 2019 17

Acceptance of Digital Signatures: A Matter of Trust 31

CAREER: Effective Trust Judgments Across Boundaries 34

Defamation in Virginia – A Merger of Libel and Slander, 47 Va. L. Rev. 1116 (1961) 25

DoD 8570.01-Manual 30

E. Encyclopedia of Law, Libel and Slander, § XV et seq. 27

Pomeroy's Equity Jurisprudence, Third Ed. § 1358; XVIII A. 27

Request for Comment 2560 of the Internet Engineering Task Force 35

Restatement (Second) of Torts § 566, Comment (b) 38

Regulations

Payment Card Industry Data Security Standard 29

INTRODUCTION

1. The undersigned movant intervenor-applicant (Sweigert) seeks the **leave of this Court** to consider this MEMORANDUM OF LAW AND ARGUMENT (**MLA**) that accompanies the MOTION FOR TEMPORAY INJUNCTION RELIEF (**MTIR**). Every effort has been made to promote judicial efficiency by clearly defining the issues this Court must be aware of, and act on, in the most efficient manner as possible.

2. ***This MOTION does not seek prior restraint against a U.S. citizen and AMENDMENT I scrutiny can be waived by the Court.*** To be blunt, David Charles Hawkins of South Surrey, British Columbia, CANADA is an extraterritorial nonresident alien. Mr. Hawkins has not demonstrated any significant connection with the community which is the United States. Pursuant to *United States v. Verdugo-Urquidez*, 494 U.S. 259 this Court need not consider any impacts on AMENDMENT I "free speech" concerning Hawkins. As the Court will learn a very precise and narrowly scoped "gag order" of sorts is suggested is enjoin the on-going, recurring and continuous broadcast of trade libel which is defamatory *per se*. A mechanism of an evidentiary hearing is suggested if Hawkins would like to provide any legally sufficient evidence (Federal Rules of Evidence) to oppose the conclusions of this pleading.

3. ***The need for an evidentiary hearing***. As a preliminary matter, pursuant to Fed. R. Civ. Proc. Rule 65(d)(C) this is a MOTION for injunctive relief, in *pendente lite*, which seeks a two-stage action by this Court (as explained below). The undersigned has distilled such a mechanism to a **Stage One** and **Stage Two** approach to this requested relief.

4. **Stage One:** The Court should explore the question "why should this Court not enjoin the Canadian resident, U.K. citizen, David Charles Hawkins, from further broadcast, dissemination and/or distribution of slander, defamatory (*per se*) opinions, trade libel accusations of malpractice, etc. targeted at the **Triple Crown** of Mr. Hawkins' slander: (1) the Federal Bridge

Certification Authority (FBCA) network, (2) those public/private partnerships connected to the FBCA network, and (3) the undersigned movant for his technical skills used in the deployment of the FBCA. Slanderous comments, accusations of criminal activity, attacks on reputations, etc. has been a recurring activity by Mr. Hawkins against entities (1) **[FBCA network]** and (2) [those entities connected to the **FBCA network**]. The undersigned (3) is fortunate that the cruel attacks on his business and trade reputation by Hawkins didn't begin in earnest until after 1/1/2019 (date provided so as not to intertwine or overlap the undersigned's federal lawsuit in the Southern District of New York (awaiting judgment for over 90 days). Mr. Hawkins is not even mentioned in the S.D.N.Y. litigation (which is focused on Racketeer Influenced and Corrupt Organizations [RICO] Act issues).

5. If Mr. Hawkins cannot provide legally enough evidence to this court in **Stage One**, then "**Stage Two**" would provide for an ORDER for injunctive relief (*pendente lite*). At such a hearing, is legally sufficient evidence tips the balance in the movant's favor (see hardship balance test below), then this Court should consider an ORDER of injunctive relief via a CEASE and DESIST (C&D) ORDER (**Stage Two**). Any such **Stage One/Stage Two** arrangement is completely left to the discretion and wisdom of the Court, it is merely presented out of an abundance of constitutional caution to comply with Fed. R. Civ. Proc. Rule 65(d)(C).

6. ***Hawkins plays a key role in a civil conspiracy violative of Va. Code Ann. § 18.2-499 and 18.2-500.*** As the Court will learn the Defendant Goodman (herein Def) is NOT the subject of this *pendente lite* relief request. It is the Def's co-conspirator (a Canadian citizen) who is the subject of this injunctive relief request. Both individuals have conspired to commit misconduct that satisfies the criteria for defamation *per se* in accordance with the jurisprudence of the Commonwealth of Virginia. At common-law defamatory words are *per se* defamatory if they

are: "(4) Those which prejudice such a person in his profession or trade," *Shupe v. Rose's Stores,* 213 Va. 374, 375-76, 192 S.E.2d 766, 767 (1972)

7. ***The Def an Hawkins have damaged the undersigned's business in a willful and malicious manner.*** In a recurring, repetitive, open-ended and on-going manner, Hawkins/Def litter the Internet with blog posts, video content, show announcements, etc. that meets the criteria of defamation per se. "Prohibiting a person from making a statement or publishing a writing *before* that statement is spoken or the writing is published is far different from prohibiting a defendant from *repeating* a statement or *republishing* a writing that has been determined at trial to be defamatory and, thus, unlawful." *Balboa Island Village Inn, Inc. v. Lemen* (2007) 40 Cal.4th 1141, the California Supreme Court. [no emphasis added]

BACKGROUND

8. The undersigned seeks protection from a Canadian community theatre actor (David Charles Hawkins) who fancies himself as a murder mystery detective (crime scene investigations [CSI]) who has teamed up with the Def to broadcast wild speculations of criminal activity and bizarre character assassinations against the undersigned to destroy the intervenor-applicant's professional reputation, trade and business. This is an open-ended cruel smear campaign that consists of:

- 5-6 hours of weekly video content discussing the movant spread across at least twelve (12) social media platforms
- 10 weekly video promotions by Hawkins which are retweeted hundreds of times by Crowdsource The Truth (CSTT) patrons

9. These excessive smear campaign products are designed to have a cumulative negative effect on the undersigned's health, career, professional reputation, trade and business reputation.

10. ***The Hawkins smear campaign against his Triple Crown of victims.*** As the Court will learn Hawkins is nothing more than an amateur actor, obsessed with homicide crime scenes, who has adopted a Sherlock Holmes alter-ego (he publishes the name "David 'Sherlock Hawkins" on several social media platforms). In sum, Hawkins performs on the Defendant's (Def's) Crowdsource The Truth (CSTT) podcasts to offer scientific sounding conclusions and determinizations to deceive the public, harm corporations and private entities and create reputational damage to the undersigned's career. This is all done by design in a reckless manner that ignores basic facts.

11. Mr. Hawkins fancies the use of legalese and has openly accused American corporations of having the "*mens rea*" to comment horrific crimes. Another favorite phrase of Hawkins is the "*inference of guilt*" bestowed upon the undersigned due to purported "*spoliation of crime scene evidence*".

12. Hawkins applies these unfounded legal characterizations to the boards of directors, government officials, employees, military officers, etc. that may orbit the **Triple Crown** of victims ((1) **[FBCA network]** and (2) [those entities connected to the **FBCA network**], the undersigned (3)).

13. ***Trade libel attacks of Mr. Hawkins on the Movant.*** In recent weeks, Hawkins has aggressively increased his trade libel attacks and defamation of the undersigned's business, trade and professional career, by offering "*evidence-based*" cyber security conclusions and determinations of the undersigned's *misconduct and malpractice*. These slurs and attacks are seemingly based on *quack research* by Hawkins to proof: that the intervenor-applicant is "hacking into systems", "installing back-doors into systems", "striping data from the crime

scene" to frustrate federal law enforcement electronic evidence forensic investigators that *may* be engaged in some unknown *investigation*, etc.

14. Hawkins enjoys lecturing to the Def's CSTT audience on the judicial *inference of guilt* applied to the undersigned for his misconduct and professional malpractice (broadcast daily to tens of thousands world-wide viewers as the last *subscriber* count on only one channel [YouTube's Jason Goodman] was **81,000+**). Hawkins has stated recently that (1) because Sweigert (undersigned) is a spoliator of electronic evidence, which obstructs federal law enforcement forensics investigators, (2) that there is the strong inference of guilt that should be applied to Sweigert (movant). No evidence to back up these *research findings, conclusions or determinations* is provided.

15. According to the part-time thespian Hawkins (who has no training or certifications in the cyber security field) electronic crime scene investigation (CSI) evidence is being destroyed by the undersigned. If such a wild claim was true it would be a violation of the professional canon of ethics of the undersigned's numerous computer security credentials to do so. This is a direct accusation of professional malpractice on the part of the undersigned.

16. ***Hawkins unqualified to render cyber security opinions.*** Several times a week the undersigned is called out by Hawkins' mis-use of cyber security vocabulary and legalese to accuse the undersigned of professional and trade misconduct, such as: (1) unauthorized hacking, (2) creating back-doors to networks, (3) social engineering with fake news, (4) conducting man-in-the-middle (MitM) attacks, (5) causing the corruption of encryption credentials, (6) destruction of crime scene evidence, (7) spoliation of evidence and (8) unauthorized use of the federal certification authority bridge to accomplish the foregoing activities (to name a few). The mis-use of professional vocabulary of the computer security industry by Hawkins is used to

assign an "*inference of guilt*". All directed at the undersigned to describe his purported malpractice and criminal misconduct using his cyber security professional knowledge.

17. Mr. Hawkins continually distributes and broadcasts his unqualified opinions (relying on the mis-use of professional computer security vocabulary) to conclude that cyber security vulnerabilities of the FBCA network were exploited by the undersigned (and others) for nefarious and criminal activities (see N.M. Rothschild, CAI Equity Partners, SERCO, Inc., National Center for Missing and Exploited Children (NCMEC), etc.). This narrative has been repeated a dozen times to a worldwide audience on CSTT; but, the narrative began on social media in 2012 when Hawkins was aligned with a "*crowdsourced investigation*" group known as Abel Danger.

18. Simply stated, in over seven (7) years of supposed Abel Dangerresearch, Mr. Hawkins has never gained even a simplistic understanding of the functionality of the FBCA network (such an explanation will be provided below). Further, Mr. Hawkins is completely unqualified to make any cyber security conclusions and determinations – but, the undersigned **IS** qualified in such matters (as recognized by the federal courts in the context of a hacking breach into a credit card processing network [*FTC v. Wydham Hotels* addressed below]).

19. The outlandish cyber security hacking narrative (smear tactic) pushed by Mr. Hawkins since 2012 is that the FBCA network has been manipulated, misused, or exploited to act as a common carrier of messages and notifications to clandestine parties concerning illegal kidnapping, dead-pool betting, murder-for-hire, and snuff film activities, etc. This type of scenario is simply not technically feasible – whether the FBCA was "hacked" or not (in this context hack means unauthorized entry into a secure computer system). Only someone who is willfully avoiding the truth and proceeding with reckless disregard to the truth could avoid

understanding the true nature of the FBCA network and the near impossibility of it operating in a manner described by Hawkins.

20. There is a timely need for an examination of the research methods of Mr. Hawkins before any more damage is done to the undersigned and innocent corporations whose only crime is that they are connected to the FBCA network and use electronic commerce.

21. ***Opportunity for Mr. Hawkins to explain his qualifications to this Court***. The undersigned suggests that a *Daubert* (*Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993)) style evidentiary hearing is needed to inquire into the Hawkins *research methods* that support his slanderous, libellous and defamatory conclusions and determinations which are widely disseminated to tarnish about the undersigned's professional ethics, his adherence to computer security codes of conduct, etc. This Court has a duty and an obligation to protect such innocents, like the undersigned, and the two dozen or so social public institutions that Hawkins has attacked in a like manner (Northrop Grumman, Boeing Aerospace, NCMEC, SERCO, Inc., National Science Foundation (NSF), Lockheed Marin, etc.).

22. The non-party (proposed defendant, ECF no. 93) Hawkins, should be compelled to offer evidence at an evidentiary hearing to explain his *research methods,* which drive his cyber security conclusions and determinations of professional misconduct and malpractice. Hawkins' methods should demonstrate how they produced *research results* that has led Hawkins to believe that the intervenor-applicant has used his skills, knowledge or experience related to the intervenor-applicant's status as an ethical hacker, Certified Ethical Hacker (**CEH**), or other computer security professional services to hack, compromise, intrude, weaken or allow others to enter into a computer network in an unauthorized manner, or caused the striping away of evidence from a crime scene – electronic or otherwise. Otherwise, such language (which is a

mis-use of professional cyber security vocabulary) should be halted from further transmission on the Internet, unless it can be demonstrated to be true – or even plausible – by Hawkins.

23. Hawkins needs to demonstrate (within the context of a suggested *Daubert*-style evidentiary hearing) how his private research methods (of no public concern), known as "CSI REVERSE ENGINEERING OF CRIME SCENES" (aka **Reverse CSI Scripts** promoted at http://ReverseCSIScripts.Com), helps him to make such stunning allegations against the **Triple Crown** (to include the undersigned, a private individual). Such an evidentiary hearing will allow the Court to evaluate whether of not such research methods amount to little more than junk science – or worse. In the highly likely event that Mr. Hawkins will NOT respond to such a request to attend such an evidentiary hearing then a default preliminary injunction could be issued at the **Stage Two** level.

24. A *Daubert*-style evidentiary hearing is recommended as it will enable an examination of Hawkins' so-called research pursuant to the spirit of Federal Rules of Evidence Rule 702. This speaks to the "General Acceptance and Admissibility for an Expert's Testimony", *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923). As Hawkins claims to be a type of expert witness "*Cambridge educated forensic economist*" (and performs his act in CSTT podcasts acting as an expert witness) his *research methods* should be examined at an evidentiary hearing to determine if these methods: (1) can they be tested with the scientific method, (2) have ever been peer reviewed, and (3) if there is general acceptance of these processes. See generally F.R.E. Rule 702. See *Nease v. Ford Motor Co.,* No. 15-1950 (4th Cir. 2017).

25. **Stage Two**: At the conclusion of such an evidentiary hearing the Court can document – once and for all – the baseless and meritless accusations of Hawkins which lack any foundation. If such a finding is made post evidentiary hearing, then the undersigned MOVES for an ORDER

FOR INJUNCTIVE RELIEF to compel Hawkins to CEASE and DESIST (C&D) any further commentary about the undersigned, the FBCA network, or public/private institutions interconnected to said FBCA network. The C&D language should forbid any future broadcast and/or podcasts, or blog entries (Twitter, Facebook, Patreon, YouTube, Stemmit, etc.) with language concerning the **Triple Crown**, (1) hacking allegations about weaknesses in the FBCA network, (2) slander and slurs directed at the public/private partnerships and private entities interconnected to the FBCA network, and (3) the intervenor-applicant, his technical competence, of trade libel accusing the movant of misconduct and malpractice.

PROCEDURAL HISTORY

26. By ORDER (ECF No. 97) all parties to this instant lawsuit are to reply and/or answer the intervenor-applicant's Second Amended (SA) Motion to Intervene (ECF No. 93). These documents are herein referenced in their entirety as if fully restated herein.

FACTUAL ALLEGATIONS

27. ***Hawkins is NOT a United States citizen***. Hawkins makes his extraterritorial (*United States v. Verdugo-Urquidez*, 494 U.S. 259) social media broadcasts somewhere near South Surry, British Columbia, Canada. To help locate the whereabouts of Hawkins it is prudent to note that he was married to the late Maren Hartwell, who apparently died from cancer on September 16, 2011. Someone named David Hawkins created a "Mary Hartwell Scholarship", announced in an Internet article on 8/15/2012. The scholarship references the date of death of Ms. Hartwell as 9/16/2011. The article on the scholarship references the White Rock Farmer's Market. Scholarship winners will apparently be announced in the White Rock and South Surrey local newspapers. There is a reference in a Cloverdale newspaper that David Hawkins ran for public office as "director of the White Rock Farmers Market, former actor in community theater

(murder and muderee).... Last book read: "A Sherlock Holmes Companion"". An address of 1702 King George Highway is provided for the candidate. Another web page lists Hawkins's phone number as 604-542-0891. A reverse look-up of the number 604-542-0891 indicates that it has been issued to Maren Hartwell of 1702 King George Highway, Surrey, British Columbia, V4A 4Z8 (Canada).

28. The web-site known as "http://ReverseCSIScripts.com" (operated by Hawkins), displays the following history of Mr. Hawkins:

- Abel Danger—From 2006 to 2018, Hawkins and Marine Corps veteran Field McConnell sponsored a web-based service for Cloud Centric CSI to help citizens reverse engineer the signature of patented weapons or weaponized patents at crime sites and solve murder mysteries of centuries past.
- From 2012 to the present, Hawkins has been operating Blending Bene and Farmers MarkIT web sites to help users to optimize their diets with 'Nutritionists Just In Time' and develop 'Chefs With Lattitude' apps to build customized recipes based on seasonal supplies in their local and regional food chain.
- Hawkins launched the 'Citizens Association of Forensic Economists' in British Columbia in 2003 as a coffee-shop based asset tracking network to monitor impact of government programs on public debt, personal assets and individual rights; to expose 'off-book' debt, combat crime and fraud and optimize the use of assets in water, energy, transport, shelter, defence, food, forestry and fisheries industries.

29. ***Hawkins transfers his rhetoric from Abel Danger to CSTT podcasts.*** Def Goodman continues to discuss the undersigned on his CSTT podcasts with Hawkins, which are distributed over a dozen social media platforms. Disparaging, slanderous, trade libellous and defaming allegations are continuously broadcast by the Def and non-party Hawkins, even after the service of the intervenor-applicant's 2A Motion (ECF No. 93) on April 12, 2019 to the Def via U.S. Priority Mail.

30. For example, in the video production entitled, "*Are EVL Teachers Hiring CAI Scrubs To Hide Signals From High Value Target & Death Pool Crime Scenes?*", April 19, 2019, at time mark 39:39, Hawkins states, "[t]he close combination of the British Patent Office and the American Patent Office takes us right to 9/11, and a number of patented devices were used in the 9/11 attack and not just in the 9/11 attack , but to actually prevent and obscure the crime scene investigation that would have led – or would have lead us – I think we are in the process of that now Jason to find the perpetrators -- and I pin that on N.M. Rothschild, uh, SERCO, and the CAI Private Equity Group, for which I believe this guy Sweigert is scrubbing busily away in that third tunnel. Over to you." [Def laughs]

31. The "third tunnel" referenced by Hawkins refers to the collage containing the unauthorized use of the likeness, portrait or image of the intervenor-applicant's face "photoshopped" on the body of a janitor below a bridge with large "SERCO" letters embedded in the wall with a schematic of the federal bridge (CertiPath diagram) next to the SERCO letters. **[EXHIBIT ONE]**.

32. These allegations of Hawkins appear to be merely lifted from an open letter to then White House Chief of Staff Gen. John F, Kelly, U.S.M.C. (ret) by the conspiracy theorist (and former partner of Hawkins) known as Field McConnell (Plum City, Wisconsin). In the 2/25/2018 letter,

McConnel writes, "[p]lease accept Brief 225 from Field McConnell – United States Marine Corps whistle-blower and Global Operations Director of Abel Danger (AD) – on **Serco's CAI private equity investors** including the late General Alexander Haig, 7th SACEUR and former director of Interneuron Pharmaceuticals, MGM Mirage, AOL and UTC and Yves Fortier, Rhodes Scholar and former Nortel director, who allegedly arranged finance for the 2010/11 start-up of Uber to develop a patentee SWAT team murder-for-hire service…". **[EXHIBIT TWO]**.

33. The Internet continues to be littered by authoritative sounding allegations and accusations, relying on the mis-use of professional vocabulary, made by Hawkins in YouTube videos, blog entries, Patreon.Com posts, etc. As previously reported in ECF No. 93 (2A Motion) the breadth of these Internet defamatory Internet posts encompasses almost a dozen social media platforms. Here, in this MOTION, the undersigned carves out the social media controlled by Hawkins – his Patreon.Com page and Hawkins controlled accounts (which does not impact the Def or his CSTT social media footprint).

34. Hawkins confirms that he considers himself some kind of Sherlock Holmes (see political candidate web-page "Last book read: "A Sherlock Holmes Companion"), as his introduction on the Patreon.Com page reads:

> A.I. Mentor **David "Sherlock" Hawkins**—inventor of the Deductive Computing Machine and the Object-Oriented Fractal Paintbrush—seeks your support for his development of Reverse CSI Storyboards, video playlists and Zulu-timed virtual reality (VR) theater to form a Virtual Production Crew with **Jason Goodman** and help students and injured communities ground truth the custodians of any patented devices which may have been used to scrub or filter crime-scene or wrongful-death data through VPN tunnels.
> [emphasis added]

35. An April 13, 2019 Patreon.Com entry states, "apparently used by Serco cut-out agents including Kevin "Mendenhall" Marsden [non-party who filed declaration with the Court] and the social engineer/ethical hacker David Sweigert to scrub tunnels under the federal bridge

certification authority network and prevent Julian Assange as a whistleblower." **[EXHIBIT THREE]**. Again, Hawkins insinuates that somehow the undersigned is "scrubbing" covert tunnels linked to the "federal bridge certification authority." Such unauthorized misconduct would be a direct violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

36. Another example occurred on April 18, 2019 **[EXHIBIT FOUR]**, "[t]he storyboards indicate that CAI investors hired social engineer/ethical hacker David "Scrubberman" Sweigert and Maxar Technologies director Joanne Isham, formerly responsible to Clinton's disgraced CIA Director John Deutsch for clandestine technical activities with the UK MOD over the federal bridge certification authority, to equip BBC scriptwriters and the EVL AI Teachers community with split-tunnel networks to prevent the U.S. Secret Service from investigating dead-pool gaming and an attempt by Serco/CAI agents to complete on 9/11 what Bernardine Dohrn and Bill Ayers started in the 1970s." The foregoing indicates that the undersigned has impeded and/or obstructed the U.S. Secret Service in some manner.

37. The trade libellous Patreon entry continues, "The storyboards suggest that Serco/CAI agents are using BBC scripts and Sweigert's split-tunnelling skills to break the chains of custody of evidence needed by the Secret Service to investigate cases of missing and exploited children (JonBenet Ramsey, Madeleine McCann!) and dismantle a patent-for-rent murder-for-hire network run by EVL Teachers..." **[EXHIBIT FOUR]**. [emphasis added]

38. The Court should note the following text "and scrubbing of files from computer was evidence of persistent bad-faith" appears in the legal white paper written by Ronald I. Raether, Jr., entitled, "Effectively Preserving Evidence", (Internet URL: https://www.troutman.com/images/content/4/7/v1/4717/RIR_EffectivelyPreservingEvidence.pdf). The entire passage reads, "*Covucci v. Keane Consulting Group, Inc.*, 2006 Mass. Super

LEXIS 313 (Mass. Sup. Ct. May 31, 2006) Court dismissed plaintiffs complaint after finding that plaintiffs deletion of e-mail and scrubbing of files from computer was evidence of persistent bad-faith repudiation of discovery obligations, intentional spoliation, and fraud on the court.". Thus, the scrubbing euphemism is considered to be a term of misconduct and evidence destruction.

39. Again, an April 16, 2019 posting states, "[t]he storyboards suggest that Serco's EVL Teachers used Clinton-sponsored dead-pool tunnels under the federal bridge certification authority to stop the US Secret Service from identifying the Sweigert brothers as the source of the dirty-bomb hoax which shut down parts of the Port of Charleston in 2017." This is the accusation of criminal activity on the part of the undersigned. **[EXHIBIT FIVE-A]**. [emphasis added] Each time Hawkins makes a Patreon.Com entry his Twitter fans are notified by recurring tweets. **[EXHIBIT FIVE-B]**

40. Another example is provided on April 14, 2019. This entry states, "with custody of Con Air AI patented devices apparently used by Serco cut-out agents allegedly including social engineer/ethical hacker David Sweigert and his brother George Sweigert to scrub data from the EVL Teachers' tunnels under the federal bridge certification authority; infiltrate saboteurs into the U.S. Navy's Space and Naval Warfare Systems Command (SPAWAR); stop the US Secret Service from recognizing BBC fake news injects in the dirty bomb hoax which shut down parts of the Port Of Charleston in 2017…". **[EXHIBIT SIX-A]**. [emphasis added]

41. Another Hawkins Patreon entry of April 22, 2019 proclaims, "[w]ith nearly 40 years' experience as an AI mentor, **I have used my Reverse CSI Storyboards** to recognize Serco's apparent use of AI algorithms to process the patented devices and systems which allegedly gave air force veteran and ethical hackers' **Red Team leader David Sweigert the capability of split tunneling data where the Bin Laden group** was able to access AWACS time-stamped ad hoc

way points needed to knock out targets in New York and Washington." **[EXHIBIT SIX-B]** [emphasis added]

42. The 4/22/2019 entry continues, "[t]he storyboards indicate that **Serco/CAI agents hired Sweigert** and Maxar Technologies director Joanne Isham, formerly responsible to Clinton's disgraced CIA Director John Deutsch for clandestine technical activities with the UK MOD over the federal bridge certification authority, and Maureen Baginski, VP Intelligence & Technical Advisory Services Senior National Security Advisor for Serco North America and former NSA Signals Intelligence (SIGINT) Director (WTF?)". **[EXHIBIT 6-B]** [emphasis added]

43. ***Hawkins abuses trademarks considered to be fraudulent activity.*** To demonstrate the legalese thrown around by Hawkins the Court should note the following phrase from an October 23, 2018 post to Hawkins' Patreon.Com blog, "[w]ith this post, and after previously trademarking "Bridge of P.R.E.Y.", David "Sherlock" Hawkins is trademarking Bridge of Pride™ and Bridge of Fraud™ to better classify his creative work on reverse CSI storyboards and associated audio-visual scripts where David attempts to identify the **mens rea** of the perpetrators who may have used SIGINT over the Federal Bridge Certification Authority (FBCA) network or its antecedents to coordinate the weapons of 9/11; HUMINT from DOJ Pride and its antecedent organisations such as the Instrument Room (Imperial Brain)." **[EXHIBIT SIX-C]** [emphasis added] caveat: a trademark for "Bridge of Pride" or "Bridge of Fraud" was not located by the undersigned in either the Canadian Trademarks Database (Internet URL: https://www.ic.gc.ca/app/opic-cipo/trdmrks/srch/home) or the U.S. patent and Trademark Office (USPTO) (Internet URL: http://tmsearch.uspto.gov/bin/gate.exe?f=searchss&state=4808:w4egna.1.1). **[EXHIBIT SIX-C]** [emphasis added]

44. As stated in the USPTO Trademark Manual of Examining Procedure (TMEP) (October 2018) (Internet URL: https://tmep.uspto.gov/RDMS/TMEP/Apr2014#/Apr2014/TMEP-900d1e1351.html):

> **906.02 Improper Use of Registration Symbol**
>
> Improper use of the federal registration symbol that is deliberate and intended to deceive or mislead the public is fraud. *See* **TMEP §906.04**.

45. The Court should note, "[t]he Trademark Manual of Examining Procedure at Section 902.03 provides that fraudulent intent and purpose in using a federal registration symbol is a basis for refusal of registration. Thus, we believe that the pending application can be opposed for registration for the above reasons. [footnote 6]". *Copelands' Enterprises Inc. v. CNV Inc.*, 945 F.2d 1563, 20 USPQ2d 1295 (Fed. Cir. 1991).

46. In a similar vein the Supreme Court recognized that the Government may regulate commercial speech to ensure that it is not false, deceptive, or misleading, *Va. Pharmacy Bd. v. Va. Consumer Council*, 425 U.S. 748 (1976) at 771-772.

47. The Government may regulate commercial speech to ensure that it is not false, deceptive, or misleading", *Va. Pharmacy Bd. v. Va. Consumer Council*, 425 U.S. 748 (1976) at 771-772. "[T]he public and private benefits from commercial speech derive from confidence in its accuracy and reliability". A listener also has little interest in being coerced into a purchasing decision. See *Ohralik v. Ohio State Bar Assn.*, 436 U.S., at 457.

48. Enough is enough. It is timely for the Court to consider a MOTION for injunctive relief to have such offending material removed from the Internet as it is the unprotected speech of a non-U.S. citizen.

LAW AND ARGUMENT

49. For a movant to be successful in obtaining *pendente lite* injunctive relief in the Commonwealth of Virginia he/she must address: (1) likelihood of irreparable harm to movant if relief IS NOT granted, (2) the likelihood of harm to the defendant is the requested relief is granted, the likelihood that the plaintiff will succeed on the merits, and (4) the public interest. See *Direx Israel, Ltd. V. Breakthrough Med. Corp.*, 952 F.2d 802, 812 (4th Cir. 1991) and *Blackwelder Furniture Co. of Statesville, Inc. v. Seilig Mfg. Co., Inc.*, 550 F.2d 189 (4th Cir. 1977).

BALANCE OF HARDSHIPS

50. When deciding whether to grant a preliminary injunction, the Court must first determine whether the movant has made a strong showing of irreparable harm if the injunction is denied, or if potential harm to the defendant (if the preliminary injunction is approved) outweighs the movant's hardships. If the balance of hardships "tips decidedly in favor of the plaintiff," *Rum Creek Coal Sales, Inc. v. Capetron*, 926 F,2d 353, 359 (4th Cir. 1991) (internal quotation marks omitted), then typically it will "be enough that the plaintiff [movant] has raised questions going to the merits so serious, substantial, difficult and doubtful, as to make them fair ground for litigation and thus for more deliberate investigation," *Blackwelder Furniture Co. of Statesville v. Seilig Manufacturing Co.*, 550 F.2d 189 (4th Cir. 1977) at 195 (internal quotation marks omitted).

51. The critical issue in a preliminary injunction case involves the balancing of the harms likely to be suffered by the parities. If the plaintiff [movant] has made a strong showing that it will suffer irreparable harm if the injunction is denied, the court must balance the likelihood of that harm against the likelihood of harm that would be suffered by the defendant.

THE IRREPARABLE HARM TO MOVANT (INTERVENOR-APPLICANT) IF THE MOTION IS NOT GRANTED

52. The undersigned is experiencing physical manifestations, from this CSTT/Hawkins smear campaign, in the form of medical treatments related to musculoskeletal symptoms of stress. These medical treatments can be directly traced to the angst created by these unqualified Hawkins conclusions and determinations that are slowly destroying the undersigned's career – all by design. The non-stop (ten (10) social media entries a week concerning the movant's professional malpractice) drum beat of trade libel and defamation per se will have a destructive cumulative impact on the undersigned, to include two (2) hours per week of CSTT "open shows" and four (4) hours per week of Patreon only pay-for-view podcast shows.

53. ***Search Engine Optimization techniques.*** Both Hawkins, and the Def have used, and are presently using search engine optimization techniques as their vehicle to integrate digital lynch mob incitements to call for more invasions of privacy, more reposts of links to defamatory vides filled with trade libel across a social media footprint that includes at least twelve (12) social media platforms (YouTube, Stemmit, GAB, Instagram, FaceBook, Twitter, etc.).

54. Hawkins has repeatedly bragged – as did a former associate of the Def "Quin Michaels", aka Korey Atkin, about his knowledge in artificial intelligence (A.I.) social media use of remote bot-nets to create the appearance of censuses amongst hundreds of users (all represent mere cyber instances of a fake electronic persona – sometimes called "sock puppet account"). Both Hawkins, and Quinn in 2018, have announced their understanding of such social media techniques. The following definition of search engine optimization (**SEO**) is provided:

> "Refers to the process of improving traffic to a given website by increasing the site's visibility in search engine results. Websites improve search engine optimization by

> improving content, making sure that the pages are able to be indexed correctly, and ensuring that the content is unique. Going through the search engine optimization process typically leads to more traffic for the site because the site will appear higher in search results for information that pertains to the site's offerings."
>
> (Internet URL: http://www.businessdictionary.com/definition/search-engine-optimization.html)

55. ***The Defamation Per Se of Hawkins' unprotected speech***. The damaging slander and trade libel that Hawkins broadcasts almost every day are direct hits on the fragile balance of a professional's career when accused of malpractice.

56. At common-law defamatory words are *per se* if they are: "(4) Those which prejudice such a person in his profession or trade," *Shupe v. Rose's Stores,* 213 Va. 374, 375-76, 192 S.E.2d 766, 767 (1972); see Note, Defamation in Virginia – A Merger of Libel and Slander, 47 Va. L. Rev. 1116 (1961); W. Prosser, Torts § 112, at 763 n. 33 (4th ed. 1971).

57. Hawkins has already met the defamation *per se* test. To illustrate. The Court is already aware of the work performed by a CISSP and/or a CISA **[EXHIBIT SEVEN]**:

> "[C]ertify that the Assessment was conducted by a **qualified, objective, independent third-party professional,** who uses procedures and standards generally accepted in the profession, **adheres to professional and business ethics, performs all duties objectively, and is free of any conflicts of interest** that might compromise the assessor's independent judgment in performing Assessments. Professionals qualified to prepare Assessments shall be: a person qualified as a Certified Information Systems Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA)..". [emphasis added]

58. Cyber security conclusions and determinations as to professional misconduct and malpractice attributed to the undersigned (by a "*Cambridge educated forensic economist*") speaks directly to the smearing of the intrinsic qualities expected of a CISSP and/or a CISA. By design, Hawkins uses several instantiations of the undersigned's name in his Patreon blog and social media entries (e.g., Dave Sweigert, David G. Sweigert, David Sweigert, etc.) to ensure maximum potential that Internet search engines will be optimized and return the results of Hawkins smears when answering the query "Sweigert ethical hacker". **[EXHIBIT NINE]** Such entries (posted ten (10) times per week) have a cumulative effect as each entry amplifies the previous entry. This creates a cumulative and compounding effect. The net effect of these Internet techniques is to create a false and overwhelmingly negative impression of the movant to disqualify him from projects that require a **CEH, CISSP or CISA**, with accompanying moral values, professional ethics and independence from conflicts of interest.

59. Hawkins has already proven himself as an expert in industrial grade smear campaign techniques, which he perfected during his Abel Danger days (2012 to 2018) to smear (1) Kristine Marcy, (2) and the same public/private partnerships connected to the federal bridge discussed in this pleading and hundreds of other innocents. Both have endured seven (7) years of non-stop slander, trade libel and defamation *per se*. Now add the movant and the Court has the **Hawkins Triple Crown.**

60. Hawkins' seven (7) year Abel Danger career is a monument to slanderous, libellous and offensive communications. The "offensive communication" of Hawkins is "capable of injuring [movant's] standing and reputation in all aspects of [his] personal and professional life, and inflicting serious psychological and emotional damage to movant]" See *Bingham v. Strave,* 184 A.D.2d 85, 89-90 (1st De't 1992).

61. A preliminary injunction is needed to protect the invasion of the movant's property interest in a technical reputation and standing in his profession from any future Hawkins allegations of trade libel misconduct and malpractice. Courts have enjoined speech if it was connected to the disparagement of a tangible property interest. See *Weiss v. Levine*, 133 N.J.Eq. 441, 32 A.2d 574; *Esskay Art Galleries v. Gibbs,* 205 Ark. 1157, 172 S.W.2d 924; Pomeroy's Equity Jurisprudence, Third Ed. § 1358; XVIII A. and E. Encyclopedia of Law, Libel and Slander, § XV et seq.

62. The movant's property right in the practice of a profession is *ex necessitate*, an intangible property, connected with the personality of a practitioner of such profession. The movant has a right to practice his ethical profession as a highly trained and certified cyber security professional – similar to any physician, attorney-at-law, or certified public accountant – free from vicous slander and trade libel.

63. In *Sloan v. Mitchell*, 113 W.Va. 506, 168 S.E. 800, it was held that the right to practice medicine was a valuable property right and the unauthorized practice of medicine by Mitchell, the defendant, was enjoined. Similarly, it has been held that the right to practice law is a property right. *Unger v. Landlords' Management Corporation*,114 N.J.Eq. 68, 168 A. 229; *Fitchette v. Taylor*, 191 Minn. 582, 254 N.W. 910, 94 A.L.R. 356; *Montgomery County Bar Ass'n v. Rinalducci*, 329 Pa. 296, 197 A. 924.

64. To amplify, in *Gazette, Inc. v. Harris,* 325 S.E.2d 713 (1985), the Supreme Court of Virginia cited, "[I]n Virginia, as in other states, the law of defamation historically has protected a basic interest. The individual's right to personal security includes his uninterrupted entitlement to enjoyment of his reputation. *Fuller v. Edwards*, 180 Va. 191, 197, 22 S.E.2d 26, 29 (1942).

"Society has a pervasive and strong interest in preventing and redressing attacks upon reputation." *Rosenblatt v. Baer,* 383 U.S. 75, 86, 86 S. Ct. 669, 676, 15 L. Ed. 2d 597 (1966)."

THIS IS NO DISCERNIBLE HARM TO THE DEFENDANT, IRREPARABLE OR OTHERWISE

65. The movant does not seek a comprehensive or over-reaching a gag order against Mr. Hawkins. The movant seeks a cessation of trade libel and comments (defamation *per se*) to protect the **Hawkins Triple Crown**, and preliminary injunctive relief can be scoped to those entities; namely (1) the movant's professional ethics or competencies (see **CEH, CISSP and CISA** discussed below), (2) the security posture of the FBCA network, and/or (3) public/private partnerships connected to the FBCA network (that is the limit of the request for and **Triple Crown** CEASE and DESIST order, to prohibit speech in those areas).

66. To demonstrate to this Court that Hawkins will suffer nothing – except embarrassment and chagrined disappointment – a sampling of Hawkins claims is herein refuted with fact-based information. Regrettably, the following explanation of the FBCA network is needed to refute the ridiculous nature and technical impossibility of Hawkins claims. The plethora of publicly available technical information about the FBCA network (which has been ignored by Hawkins) speaks to reckless disregard and willful blindness to the truth.

67. ***The truth about the FBCA network.*** Solid technical information about the impossibility that the operation of the FBCA network could be hijacked by clandestine and nefarious parties is consistently ignored by the so-called "*Cambridge educated forensic economist*" actor, who enjoys performing with his Sherlock Holmes alter-ego recurring CSTT podcasts with the Def. By hiding behind legalistic sounding expert witness-ish credentials, Hawkins casually proclaims that the FBCA network can be easily hacked by somehow exploiting weaknesses – namely by

the intervenor-applicant (who else?). David "Sherlock" Hawkins (as he enjoys calling himself) continues to dispense conclusions and determinations about the FBCA network, the entities connected to it, and especially the movant as he worked on it. The **Triple Crown** of slander for Mr. Hawkins.

68. Mr. Hawkins cannot provide evidence of his research findings to support his allegations against the undersigned and innocent public institutions (SERCO, Inc, NSF, NCMEC, etc.). At the core to all these allegations is the federal bridge certification authority (FBCA) network. It is technically impossible for the FBCA network to enable the outlandish hacking attacks claimed by Hawkins and he has no proof or research results that would indicate otherwise.

69. ***Movant source of qualified opinion to rebut Hawkins.*** The undersigned has been certified by the same professional bodies which have been recognized by the federal courts to provide expert assistance in matters such as the security of network vulnerabilities that may reside within an FBCA type of network. The Court's attention is called to the STIPULATED ORDER FOR INJUNCTION issued 12/11/2015, ECF no. 283, *Federal Trade Commission v. Wyndham Worldwide Corporation*, et. al., 2:13-CV-01887-EAS-JAD. U.S.D.C., Dist. of New Jersey. **[EXHIBIT SEVEN]** (See Internet URL: https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation).

70. In *FTC v. Wyndham* the court ordered that annual reports were to be made considering the integrity of the computer networking environment of the hotel chain, which previously was held responsible for the data breach of 10,000 consumer credit cards and cardholder information. On page 6 of 18 of said ORDER **[EXHIBIT SEVEN]** the court mandated 20 (twenty) years of cardholder data assessments. Such assessments would be required to be carried out against the comprehensive Payment Card Industry Data Security Standard (PCI DSS) Risk Assessment

Guidelines. Further such assessments had to be performed by qualified experts. At para. II.3, pg. 7 of 18, the court stated:

> "[C]ertify that the Assessment was conducted by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession, adheres to professional and business ethics, performs all duties objectively, and is free of any conflicts of interest that might compromise the assessor's independent judgment in performing Assessments. Professionals qualified to prepare Assessments shall be: a person qualified as a Certified Information Systems Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA).".

71. The undersigned is certified as both a CISSP and a CISA. Therefore, the undersigned is qualified to speak to issues of risk assessments, vulnerabilities, malware, computer hacking and other topics of interest to this Court – not Mr. Hawkins. Caveat: both the CISSP and the CISA are recognized credentials as part of the U.S. Department of Defense cyber defense program (DoD 8570.01-Manual).

72. ***Fact-based analysis of Hawkins claims.*** A qualified cyber security opinion would conclude that it is nearly impossible for components of the FBCA network to be used for the transmission of covert message payloads as suggested by Hawkins. The federal bridge acts as a validation authority of the status of digital certificates, much in the same manner as a credit card "clearinghouse" routes card status messages and requests to an issuer bank (known host) via a complex interconnected card payment processing network (nearly identical to the FBCA network). Digital certificates, like credit cards, require their current status to be verified; status as to valid, expired, revoked, unknown, etc. **[EXHIBIT TEN-A]**

73. The Court should consider an illustration from the web-site of IdenTrust, which offers the following explanation of FBCA functionality:

> **Providing government trust based on cross-certification with the U.S. Federal Bridge Certification Authority (FBCA)**
>
> IdenTrust Global Common (IGC) certificates are cross-certified with the U.S. Federal Bridge Certification Authority (FBCA), enabling trust and interoperability with a wide range of systems and applications. IGC Certificates are ideal for use by U.S. federal and state governments, contractors, healthcare providers and enterprises where a high degree of trust and interoperability is desired. Leveraging more than a decade of expertise in identity-proofing and providing authentication credentials, the IdenTrust Global Common (IGC) PKI provides certificates from Basic Assurance certificates to PIV-I credentials.
>
> (Internet URL: https://www.identrust.com/certificates/federal-bridge-certified)

74. Much like in the FBCA network, in the credit card verification and validation network, the issuing bank acts as the final arbitrator of the status of such card, and then approves a pending transaction (based on the success of the "status" responder). In a like manner, the issuing agency of a digital certificate (dig-cert) has the final authority to validate the status of a dig-cert (valid, expired, revoked, etc.).

75. To illustrate, Matthew J. Stifel explained in the article *Acceptance of Digital Signatures: A Matter of Trust*, 21st Computer Science Seminar, **[EXHIBIT TEN-B]**, quoted in relevant part:

> " Many companies and government agencies issue electronic credentials within their own domain. It is unrealistic that a single global issuer of these credentials will ever exist. Many of the

> public and private entities issuing electronic credentials are doing so with the use of Public Key Infrastructure (PKI) technology. In order for these credentials to be trusted so that a digital signature can be validated between two entities, a higher level architecture (trust model) must exist.
>
> The US Federal Government has developed an architecture to extend trust beyond a single trust domain. The Federal Bridge Certificate Authority is an example of this type of infrastructure element. The Federal Bridge CA, operated by the General Services Administration (GSA), provides cross certification among trust domain PKI's. The Federal Bridge acts as a trust conduit. It does not provide a root of trust, but actually "links together" existing trust infrastructures by mapping their "policies".

76. Note: A digital signature is an application of technology for signing an electronic message that ordinarily provides the highest degree of assurance for identifying the signer. Digital signatures are a subset of electronic signatures, but unlike other electronic signatures, digital signatures are cryptographically derived, i.e., backed by a process such as a public key infrastructure (PKI). A digital signature enables legally binding transactions via non-repudiation. The recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.

77. To continue the credit card authorization system analogy, even if a card purchaser (cardholder) is using a Visa (brand owner) credit card, by relying on the electronic payment clearinghouse (acquirer), the Visa card can still be verified and validated by the interconnection of several major credit card brands that act in a cooperative manner to provide verification and validation services in near split-second time. The purpose of such activity is to deny purchases to revoked and expired credit cards. The issuer bank (like the issuer of a dig-cert) would deny the purchase if a card is revoked or expired and return the notification to the merchant (relying party in the FBCA network). The FBCA is a "clearinghouse" of sorts.

78. The digital certificates that are widely used throughout the federal government, work on the same principle when it comes to the process of validating that the dig-cert has not been revoked or expired. A routing protocol has been designed which follows a known networking path to the issuer of the digital certificate (known host server) to verify and validate the status of said digital certificate. If the issuer of the digital certificate has no expired or revoked status associated with the credential, a response message with dig-cert status is returned to the federal bridge (acting as clearinghouse acquirer) for further routing to the next hop. When the federal bridge receives the dig-cert status response message it has the proper routing and path validation software to ensure that the appropriate agency application is notified of the positive status of the credential.

79. This type of procedure allows for the processing of valid credentials that represent the status of the user's dig-cert credential. In the case of the federal bridge, interconnected certification authorities that are maintained by issuers of certain digital certificates, such as Boeing, Northrop Grumman, Certipath, Entrust, etc., can quickly validate the status of other company credentials. This facilitates inter-company electronic commerce. Pursuant to the 2000

Electronic Signatures in Global and National Commerce Act (E-Sign Act) parties can agree on authentication and authorization of legally binding transactions (equivalent to a "wet" signature [traditional pen and ink]). Therefore, the use of the federal bridge can expedite electronic commerce by facilitating the execution of legally binding transactions in a fast and exhibition expeditious manner. In sum, the FBCA network facilitates electronic commerce and streamlines legally binding transactions between the government and public/private partners.

80. To illustrate, the National Science Foundation research project, *CAREER: Effective Trust Judgments Across Boundaries,* is quoted in relevant part:

> Increasingly important social processes are migrating to an increasingly decentralized, inter-organizational information infrastructure. This work investigates the resulting trust issues. Are there grounds for one entity, Alice, to trust a remote entity Bob, with a particular task? When such grounds exist, how can this information be securely transmitted across the boundaries that separate Bob from Alice? Do Alice's applications and tools enable her to make the appropriate trust judgment?
>
> This research begins with the technology of public key infrastructure (PKI), because it can communicate assertions without sharing secrets, and trusted computing platforms, because of they can potentially create islands of trust within a distributed infrastructure."
>
> **[EXHIBIT EIGHT]**

81. The key here is that public key infrastructure (PKI) communicates assertions (dig-cert status [valid, revoked, expired]) **WITHOUT** communicating the clandestine covert message payload that Mr. Hawkins fancies. It is simply not possible. Mr. Hawkins' allegations about hacking the FBCA network to transmit covert and clandestine instruction messages (covert

payload) to nefarious actors is almost technically impossible. Further, Mr. Hawkins is completely unqualified to make such statements.

82. The computer networking protocol that is relied upon to validate dig-cert status is known as the Online Certificate Status Protocol (OCSP). A relevant tutorial is provided by the web-site operated by "digicert", quoting in relevant part:

> "An OCSP request is a signed message. It consists mainly of two components: a request body, and an optional signature block. The request body contains one or multiple certificate status requests. The body consists of the following fields:
>
> Version – OCSP Request version number. It is default to v1.
>
> Requestor name – optional field
>
> One or more requests – web server only include one certificate status request per OCSP request message.
>
> Extensions – This optional field to include extra information which may be communicated between the client and the OCSP server, such as the expected OCSP response message type from the client, nonce, or archive cutoff date, etc."
>
> (Internet URL: https://community.digicert.com/en/blogs.entry.html/2015/02/27/what-is-ocsp.html)

83. OCSP was first conceptualized via *Request for Comment 2560 of the Internet Engineering Task Force* (IETF), June 1999. Quoted in relevant part:

> 2.1 Request
>
> An OCSP request contains the following data:
>
> -- protocol version
> -- service request

> -- target certificate identifier
> -- optional extensions which MAY be processed by the OCSP Responder
>
> Upon receipt of a request, an OCSP Responder determines if:
>
> 1. the message is well formed
>
> 2. the responder is configured to provide the requested service and
>
> 3. the request contains the information needed by the responder If any one of the prior conditions are not met, the OCSP responder produces an error message; otherwise, it returns a definitive response.
>
> (Internet URL: https://www.ietf.org/rfc/rfc2560.txt)

84. The OCSP standard, IETF RFC 2560, has **limited the message length and content** of an OCSP Request message and Responder message; with OCSP dig-cert status returned via OCSP Responders (analogous to the issuer bank in the credit card processing network model). Mr. Hawkins needs to explain where exactly a covert and/or clandestine payload message can be inserted into an OCSP message used by the FBCA network. It can't.

85. The size of the OCSP transaction messages that are routed through the federal bridge are very lightweight and small. Many electronic mail systems can carry payload attachments up to the size of 10 to 15 megabytes. This is not the case with an OCSP transaction verification messages. Such authorization messages are purposely designed to be very short and small to allow for quick processing and reduced network latency. Otherwise bulky messages would clog the network and response times would be in the minutes, instead of seconds.

86. The Court should note that all the foregoing references are publicly available on the Internet. Easily accessible to Mr. Hawkins. It is Mr. Hawkins who has slung allegations against the FBCA network and those entities connected to it since 2012. Yet, in all this time Mr. Hawkins has not undertaken even the most basic research that has been presented above. This is

the sum of Mr. Hawkins' seven-year research undertaking (death march) to *study* the FBCA network and the entities connected to it – nothing. There is nothing to base his wild, stunning, defamatory, libellous and slanderous accusations on. There is no pathway for clandestine and nefarious lesbian operatives can transport orders of cover t snuff films via clandestine channels on the FBCA network. Not any more than a credit card reader could read a covert and clandestine Visa card to send messages to saboteurs, accomplices, pedophiles or any of the other FBCA network bogey men created in the mind of Mr. Hawkins.

87. If a preliminary injunctive order prevents Mr. Hawkins from discussing the movant, movant's technical capabilities, movant's background with the federal bridge, the FBCA network itself, and interconnected FBCA network entities Mr. Hawkins will lose nothing.

LIKELIHOOD OF SUCCESS

88. The undersigned has the ability to disqualify the hacking and professional malpractice notions and other wild speculations of Hawkins. The Court has learned that the undersigned is a Certified Ethical Hacker (CEH), and a CISSP and a CISA and is well qualified to neutralize and make moot the outrageous and unqualified opinions of Mr. Hawkins. The undersigned can speak to these issues (cyber security) from a professional platform – Mr. Hawkins cannot. This creates a clear advantage for the movant in addressing the uneducated guess work of Hawkins.

89. As explained in the Memorandum of Law that accompanied the SA Motion to Intervene (ECF No. 93) [herein cited and referenced as if fully restated] Hawkins' acts of falsely imputing criminal acts and trade libel (professional reputational damage) to the undersigned is *per se* defamatory. *Mazurek v. Armstrong* (96-1104), 520 U.S. 968 (1997).

90. Under Virginia law, it is defamation per se to make false statements which "prejudice [a] person in his or her profession or trade." *Great Coastal Express v. Ellingon*, 230 Va. 142, 334

S.E.2d 846, 849 (1985). For such prejudice to arise, the statements must relate to "the skills or character required to carry out the particular occupation of the plaintiff." *Fleming v. Moore*, 221 Va. 884, 275, S.E.2d 632, 636 (1981). In addition, if the movant (undersigned) establishes a claim for defamation per se, Virginia law presumes that the plaintiff [movant] suffered actual damage to his/her reputation and, therefore, does not have to present proof of such damages. *Fleming*, 275 S.E.2d at 636.

91. Mr. Hawkins' statements imply the existence of fact and are not "pure" opinion. Statements clearly implying the existence of facts are actionable as defamation. *Oliman v. Evans*, 750 F.2d 970, 982 (D.C. Cir. 1984); Restatement (Second) of Torts § 566, Comment (b) (statements that imply the existence of facts that would justify the opion constitute "mixed opinions" are are subject to defamation claims). As the Supreme Court noted, "simply couching statements in terms of opinion does not dispel the impliatons [of fact], and the statement ... can cause as much damage to reputaton as [factual assertions]." *Milkovich v. Lorain Journal Co.*, 497 U.S. 1, 19, 110 S.Ct.2695, 2706, 111 L.Ed.2d 1 (1990). Thus, because "[i]t is for the court, not the jury, to determine as a matter of law whether an allegedly libellous statement is one of fact or one of opinion. *Slawik v. News-Journal*, 428 A.2d 15 (Del.1981); *Catalano v. Pechous*, 69 Ill.App.3d 797, 25 Ill.Dec. 838, 387 N.E.2d 714 (1978); *Rinaldi v. Holt, Rinehart & Winston, Inc.*, 42 N.Y.2d 369, 397 N.Y.S.2d 943, 366 N.E.2d 1299 (1977)." *Chaves v. Johnson*, 335 S.E.2d 97 (1985) at 102 (Supreme Court of Virginia).

PUBLIC POLICY

92. ***Hawkins has no Amendment I protection.*** The extraterritorial resident of Canada Hawkins (who is not a U.S. citizen) has no expectation of privileges derived from AMENDMENT I of the U.S. Constitution. Hawkins creates his content in Canada, and then

posts his outrageous slanderous allegations on Internet network servers (such as Patreon.Com, Twitter, GAB, Facebook.COM, etc.). This Court should not be encumbered with AMENDMENT I concerns over Hawkins slanderous, libellous and defamatory "free speech" – which is unprotected. Further, pursuant to *United States v. Verdugo-Urquidez*, 494 U.S. 259 Hawkins has NO expectation of AMENDMEMT I protection (the court contending that "the people" intended to be protected by the Fourth Amendment were the people of the United States, and that the defendant's "legal but involuntary presence" on U.S. soil (a direct result of his arrest) failed to create a sufficient relationship with the U.S. to allow him to call upon the Constitution for protection).

93. ***Hawkins' speech is "Commercial Speech".*** The Patreon.Com blog pages of Hawkins is riddled with solicitations for financial assistance in the development of the "reverse-engineered CSI storyboards". Hawkins' non-sense about his "reverse CSI scripts" is a commercial enterprise and qualifies as commercial speech. The Supreme Court addressed the restriction of commercial "free speech" in *Central Hudson Gas & Electric Corp. v. Public Service Commission Of New York*, No. 79-565, 447 U.S. 557; 100 S. Ct. 2343; 1980 U.S. LEXIS 48; 65 L. Ed. 2d 341; 6 Media L. Rep. 1497; 34 P.U.R.4th 178, June 20, 1980., finding:

> "The Constitution therefore accords a lesser protection to commercial speech than to other constitutionally guaranteed expression. 436 U.S. at 456, 457. The protection available for particular commercial expression turns on the nature both of the expression and of the governmental interests served by its regulation.
>
> And
>
> Although the Constitution accords a lesser protection to commercial speech than to other constitutionally guaranteed expression, nevertheless the First Amendment protects

commercial speech from unwarranted governmental regulation. For commercial speech to come within the First Amendment, it at least must concern **lawful activity and not be misleading**. Next, it must be determined whether the asserted governmental interest to be served by the restriction on commercial speech is substantial. If both inquiries yield positive answers, it must then be decided whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest. Pp. 561-566" [emphasis added]

94. The *Central Hudson* majority went on to develop a four-part analysis commensurate with the supposed intermediate status of commercial speech. Under that test, a court reviewing restrictions on commercial speech must first determine whether the speech concerns a lawful activity and is not misleading. If the speech does not pass this preliminary threshold, then it is **not protected by the First Amendment at all**. *Id.*, at 566.

95. ***Protection of innocent institutions.*** Public policy supports the issuance of injunctive relief and a temporary restraining order. Mr. Hawkins has not only slandered the undersigned with trade libel causing damage to the undersigned career and professional reputation, but Mr. Hawkins has also slandered dozens of American corporations and institutions. These libellous, slanderous, and defamatory accusations and allegations, which appear to have no foundation and are meritless, have been targeted at Northrop Grumman, Lockheed Martin, Boeing Aerospace, Motorola, Serco, Inc., the National Center for Missing and Exploited Children (NCMEC), various departments of the United States government, U.S. Department of Justice, US Marshals Service, etc.

96. These institutions and organizations deserve the same protection that is now being requested by the undersigned. The Court should consider its public duty to protect such

innocents and conduct an adequate review of the scientific and research methods claimed by Mr. Hawkins. The findings of the so-called *research methods* that have led Mr. Hawkins to claim that he has evidence that implicates the aforementioned corporations with participation in hacking the federal certification authority bridge, planning of the 911 disaster, extortion of government officials through kiddie porn, creation of snuff films, kidnapping of children, etc.

97. The U.S. Supreme Court enunciated the principle that the State may intervene to protect the public from harmful commercial speech in *Ohralik v. Ohio State Bar Assn.*, 436 U.S. 447 (1978) at 462 by stating that:

> "the State has a legitimate and indeed 'compelling' interest in preventing those aspects of solicitation that involve fraud, undue influence, intimidation, overreaching, and other forms of 'vexatious conduct …
>
> and
>
> [the State had] "a strong interest in adopting and enforcing rules of conduct designed to protect the public." Id., at 464

98. Public policy supports that these important institutions and organizations should be protected from such slanderous, outrageous, and reprehensible unfounded allegations – which appear to be little more than rehashes of previous Abel Danger blog posts from a decade ago. Such stains on reputations cannot be easily removed once they had been repeated over and over and over by the likes of Hawkins and his Abel Danger gang stalking crowd. These horrendous allegations (based on *evidence* collected by a community theatre actor and Abel Danger "*Cambridge educated forensic economist*") are tweeted and retweeted throughout the day to expand the exposure of these insinuations in a widely distributed manner across a dozen social media platforms, having a cumulative impact.

99. The continued, open-ended broadcast and maintenance of these horrific allegations will only cause a plethora of negative impacts on society as a whole. For example, these allegations could seriously impact stockholder relationships with the targeted corporations, as Mr. Hawkins so fondly accuses the stockholders of responsibility for the wrongful deaths on 9/11 because of their so-called *patent influence* from Serco Incorporated, headquartered in Virginia.

100. ***Public policy supports enabling electronic commerce***. Hawkins is having a chilling effect on the adoption of trusted electronic commerce to support legally binding transactions with the federal government. The FBCA network supports the efficient flow of official regulatory and governance related document submissions between government agencies and private/public partnerships that are legally binding. The FBCA network has eliminated the costly need for "wet" signatures on source documents that may the be sent via overnight courier and lost in mail room intake. The FBCA network dramatically brings economies of scale and computer networking efficiency by providing for a legally binding and legally sufficient digital nature. Caveat: A "wet" signature is a traditional pen-and-ink signature.

101. The FBCA network supports many e-government initiatives; such as the 2000 Electronic Signatures in Global and National Commerce Act (E-Sign Act), the Government Paperwork Elimination Act (GPEA), Public Law 105-277 (codified at 44 U.S.C. 3504), OMB M-00-10: OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act (April 25, 2000), National Archives and Records Administration: Records Management Guidance for Agencies Implementing Electronic Signature Technologies (October 18, 2000), E-Government Act of 2002, Public Law 107-347, Federal Information Security and Modernization Act of 2014, Public Law 113-283, Department of Justice: Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies (November 2000), U.S.

Department of State Guidebook for the Implementation of Electronic Signatures,, National Institute of Standards and Technology (NIST) SP 800-63, Electronic Authentication Guideline, to name a few.

102. Unfortunately, every week another corporation is implicated in a plot to operate this murder for hire network – simply because their institutions are connected to the FBCA network. Thanks to Hawkins, every new private company and/or public institution considering connection to the FBCA network must weigh the risk of being included in the Hawkins story line of snuff films, child abductions, lesbian federal agents, etc. all whom apparently utilize the FBCA network for their nefarious criminal deeds. The mere technical connection to the FBCA network appears justification enough for Mr. Hawkins to aim criminal allegations at boards of directors, employees, stockholders, etc. Allowed to continue, this horrific slander – and the possibility of being included in the story line – will only dampen the adoption of the FBCA network and digital signatures by those companies and institutions that can benefit from this service. The continued, open-ended and on-going slander campaign to disparage the FBCA network (and the undersigned and private corporations) frustrates, impedes and obstructs public policy.

103. ***Hawkins's unprotected speech is of no social consequence***. Hawkins has a long history of creating digital lynch mobs with his industrial smear campaigns (Abel Danger, 2012 – 2018). The drivel, prattle, conspiracy hoaxes, rumors, conjecture, outright slander, defamation *per se* and the libel of Hawkins damages individuals, corporations and public/private partnerships. But his drivel – even taken at face value -- is of little or no social consequence. As the Supreme Court explained in *Virginia v. Black*, 538 U.S. 343, 358 (2003), "[t]he First Amendment permits restrictions upon the content of speech in a few limited areas, which are 'of such slight social

value as a step to truth that any benefit that may be derived from this is clearly outweighed by the social interest in order and morality.'"

SUMMARY

104. Hawkins shows no sign of de-escalating his reprehensible and stunning allegations, accusations and insinuations – all are damaging to the technical trade, reputation and career of the undersigned. Mr. Hawkins is unqualified to make any allegations concerning "hacking activities" that purportedly rely on the FBCA network.

105. Mr. Hawkins has not been able to prove that it is even theoretically possible to "hack" into the FBCA network. It is almost inconceivable and highly improbable that the federal bridge messaging store-and-forward system (using short credential messaging packets of 32 to 64 bits in length) could be used to transmit a payload of clandestine messages. Mr. Hawkins has the burden to demonstrate that he understands the critical infrastructure of the FBCA network and that he has been able to determine flaws, vulnerabilities, and weaknesses that could be exploited in the manner that he describes, namely the payload transport of clandestine messages – or other hacks carried out by the undersigned.

106. Of course, this begs the question as to why nefarious criminals would go to such great lengths as to use a highly regulated, highly accredited, highly visible, and highly secure system such as the FBCA network. The FBCA network relies on the highest levels of security, as described in the certification path validation which requires the confirmation of specific network routes (hops) to the issuer of the digital certificate in question. In other words, specific paths (routes, hops) are validated to ensure only specified Internet electronic pathways are used to connect to dig-cert status responders. This is remarkably security.

107. It is the insinuation, indirect attacks, and direct attacks of the undersigned by Mr. Hawkins, who uses his expert witness classification as a "*Cambridge educated forensic economist*", to disparage, destroy, harm, and injured the professional reputation of the undersigned. Mr. Hawkins drives his slanderous sword directly into the professional heart of the undersigned, by questioning professional ethics, professional practice and procedures, best industry practices for his craft, and other issues related to the career and profession.

108. These facts should be memorialized, ratified and verified by a court of competent jurisdiction (this Court) and so stated in an authoritative court judgement. The reverse is true, if no evidence can be presented to support these stunningly slanderous claims then that fact should also be so stated.

RELIEF REQUESTED

109. Based on the foregoing, and the accompanying Memorandum of Law, this Court should issue a temporary CEASE and DESIST (C&D) ORDER directed at the non-party David Charles Hawkins. Conditions of such an ORDER should include:

- The immediate halt to any future appearances by Mr. Hawkins on the Def's CSTT podcast shows in any form and for any reason.
- The immediate halt to any future Internet blog posts, Patreaon.Com entries, Twitter tweets, GAB updates, Facebook entries, BitChute entries, or any other social media platforms, that discuss, comment or critique the intervenor-applicant's technical profession, computer security expertise, ability to conduct risk assessments, or any other facet connected, directly or indirectly, with allegations about hacking, installing back-doors, breaching of system security, allowing for vulnerabilities and weakness, etc.

- An immediate halt to any future podcast, distribution of opinions, or podcast shows that comment on any institution or corporation that is interconnected to the FBCA network. This includes any technical characterizations related to any facet connected, directly or indirectly, with allegations about hacking, installing back-doors, breaching of system security, allowing for vulnerabilities and weakness, etc.
- The immediate halt to the expression of opinion, podcast broadcast, descriptions of activities, or any other commentary about the undersigned and any associated technical projects, former employers and technical journals published by the undersigned. This includes commentary about the undersigned's involvement with the U.S. Air Force, Booz*Allen & Hamilton, EnTrust Technologies, U.S. Army STRICOM and the FBCA network.
- The ORDER should include a request for the voluntary cooperation of all social media platform providers utilized by Mr. Hawkins, requesting that his channel content be reviewed for potential violations of any Terms of Service, User Acceptance Agreements, Terms of Use, etc.

110. The relief requested only enables one private person [undersigned] to curtail the broadcast of unqualified determinations of another private person [Hawkins] about a matter that is not of public interest (Hawkins' Reverse CSI Engineering concepts). The Court should note that Mr. Hawkins is not a member of any media, advocacy, public interest or news-gathering organization.

I certify that all of the foregoing information is truthful and not submitted for any other purpose than for adjudication of the claims contained within. This certification is provided under the penalties of perjury on the 26th day of April 2019.

Respectfully submitted,

Pro Se Party D. George Sweigert, c/o
P.O. Box 152
Mesa, AZ 85211
Spoliation-notice@mailbox.org